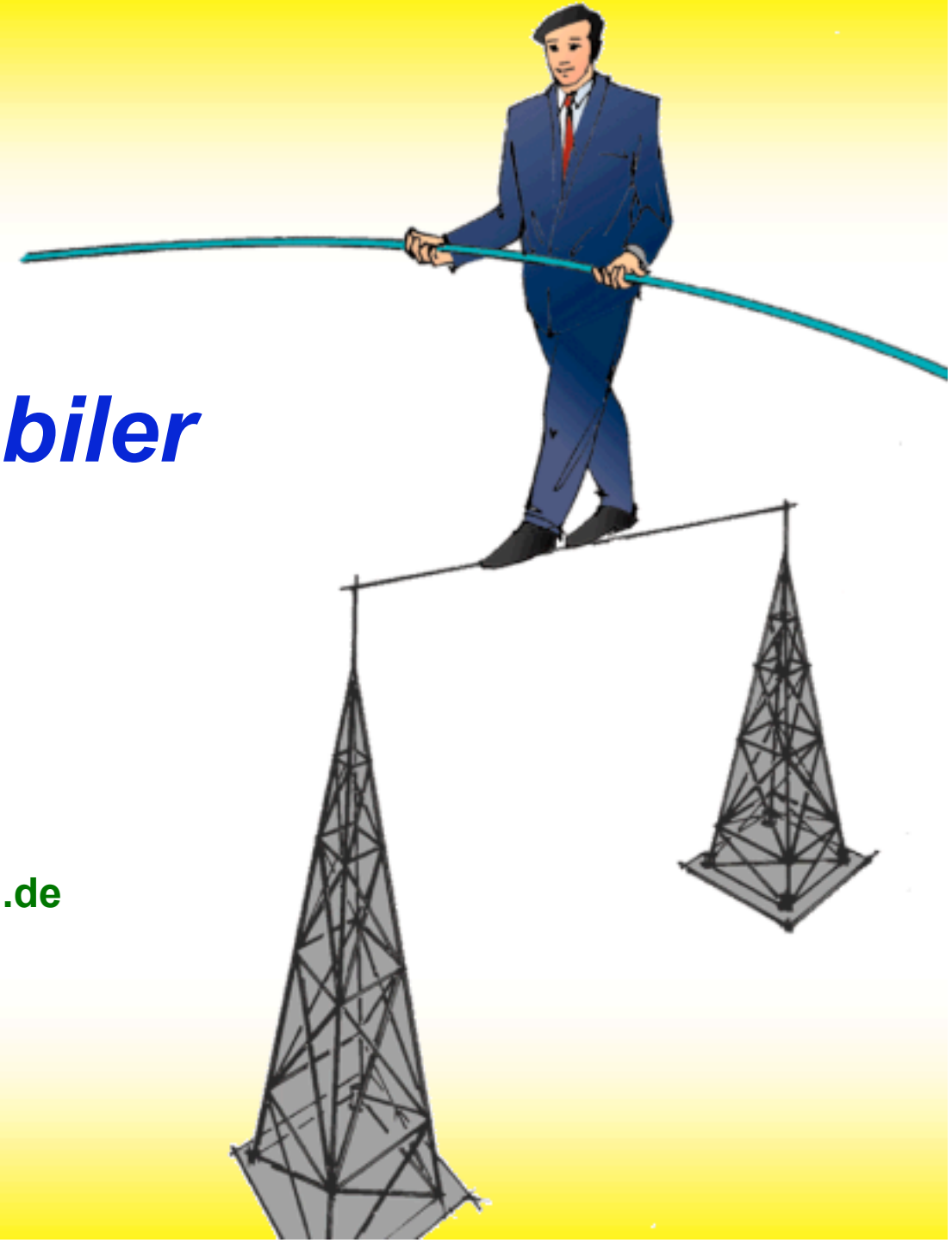
Sicherheit mobiler Systeme



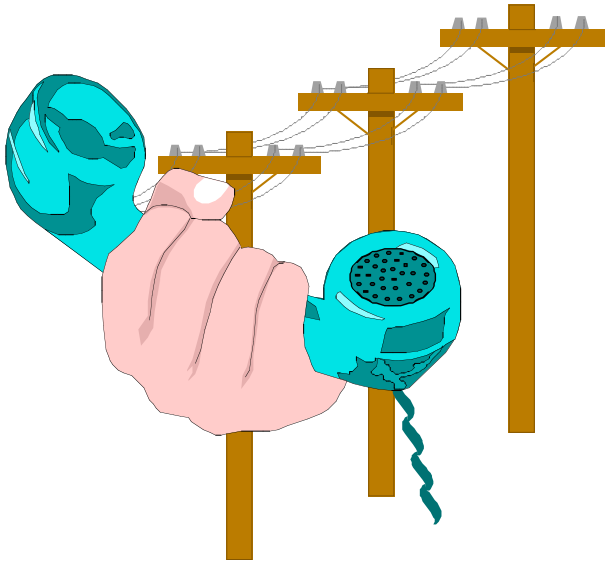
Hannes Federrath

Universität Regensburg

http://www-sec.uni-regensburg.de

Mobilkommunikation – Einführung

- ***Unterschiede Festnetz- und Mobilkommunikation***
  - Teilnehmer bewegen sich
  - Bandbreite auf der Luftschnittstelle knapp
  - Luftschnittstelle störanfälliger als Leitungen des festen Netzes:
    - zeitweilige Diskonnektivität
  - Luftschnittstelle bietet neue Angriffsmöglichkeiten:
    - erleichterte Abhörmöglichkeit
    - Peilbarkeit



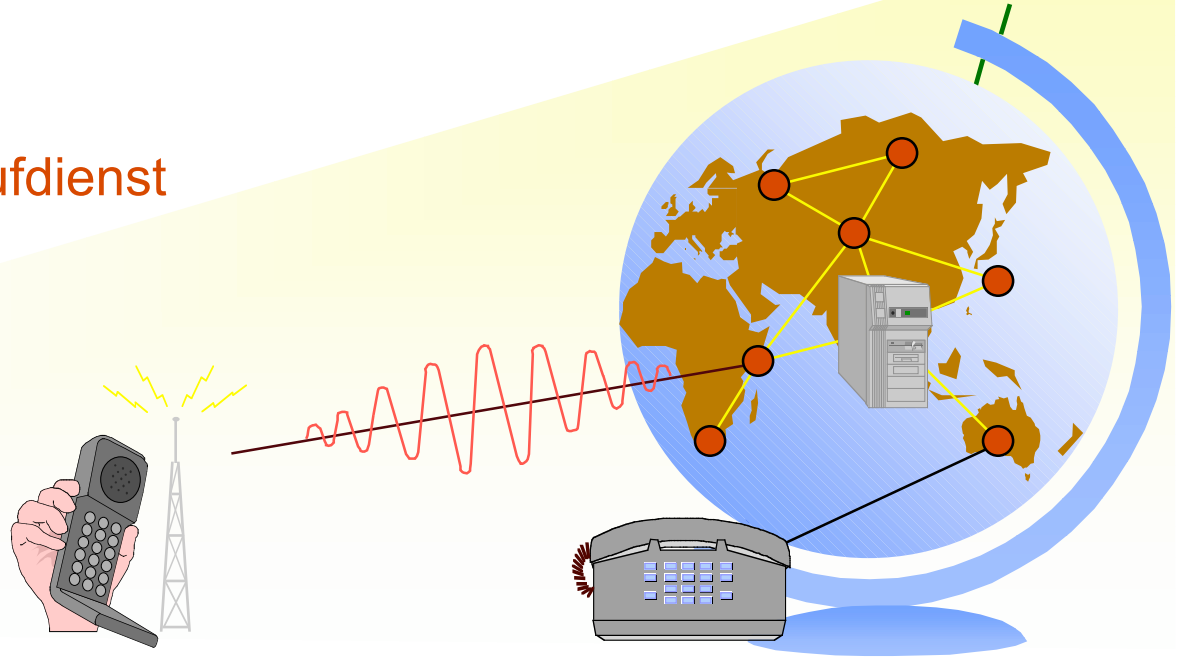
Mobilkommunikation am Beispiel GSM

– Ursprünglich: Groupe Spéciale Mobilé der ETSI

- ***Sicherheitsfunktionen des Global System for Mobile Communication***

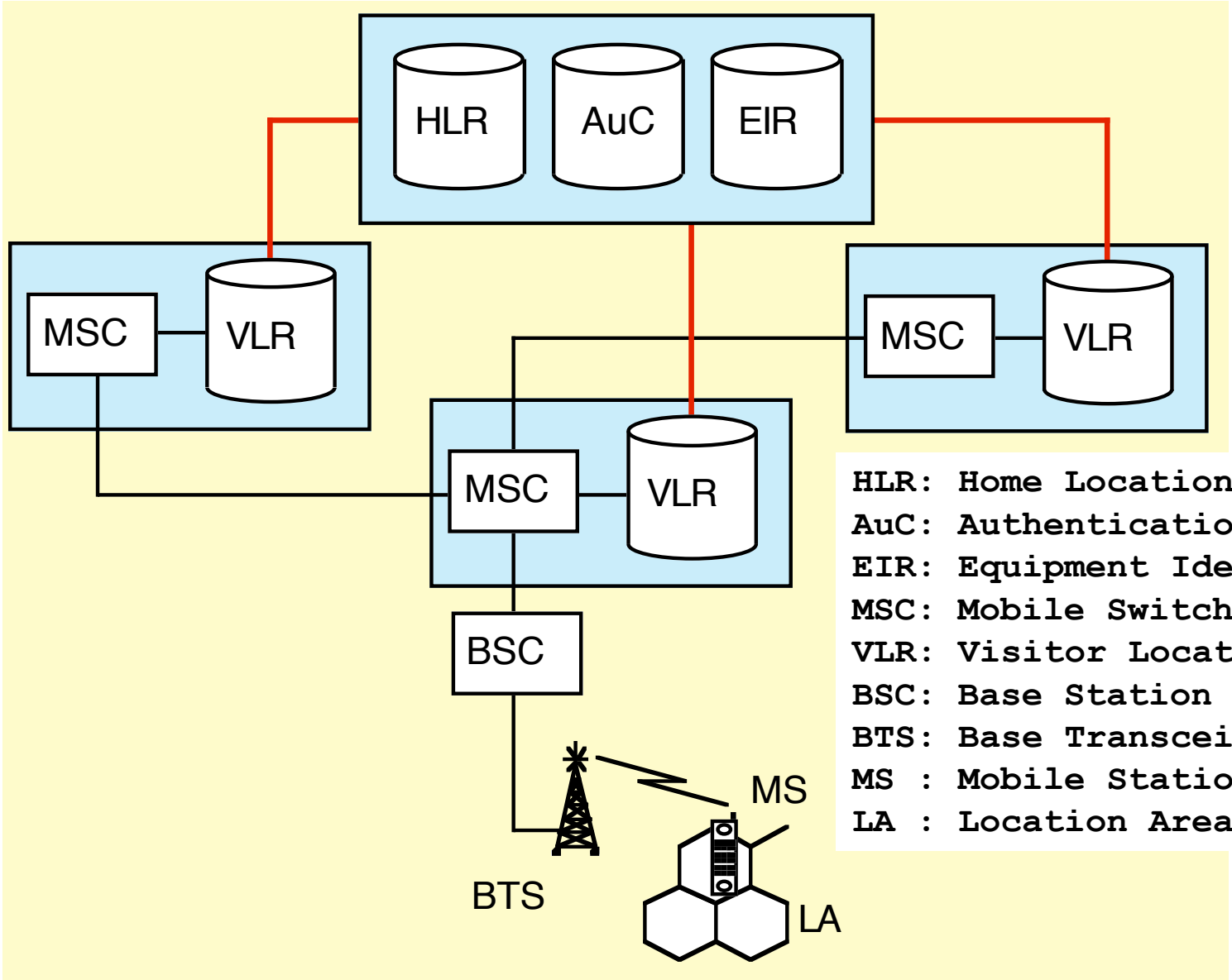
  - Zugangskontrolldienste (PIN, Chipkarte)
  - Authentikations- und Identifikationsdienste
  - Unterstützung von temporären Identifizierungsdaten (Pseudonymen)
  - Abhörsicherheit für Outsider auf der Funkschnittstelle

  - priorisierter Notrufdienst



Struktur von GSM

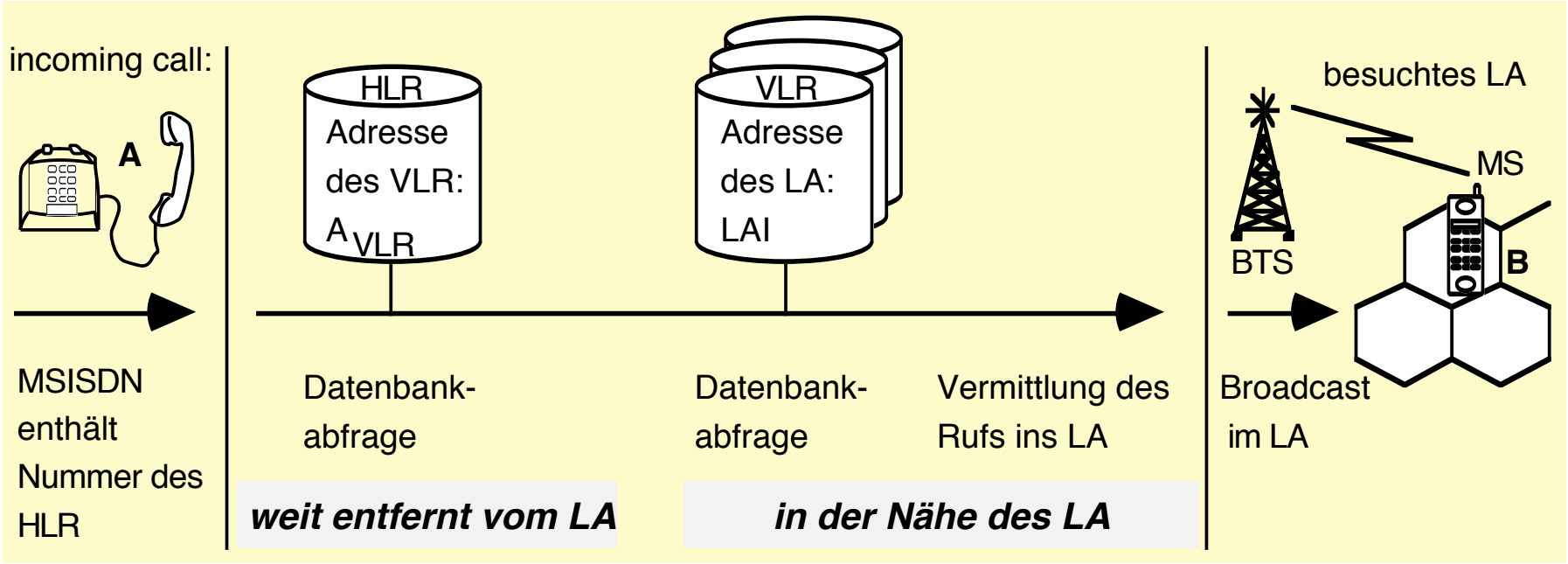
- *Logischer Netzaufbau*



HLR: Home Location Register
AuC: Authentication Center
EIR: Equipment Identity Register
MSC: Mobile Switching Center
VLR: Visitor Location Register
BSC: Base Station Controller
BTS: Base Transceiver Station
MS : Mobile Station
LA : Location Area

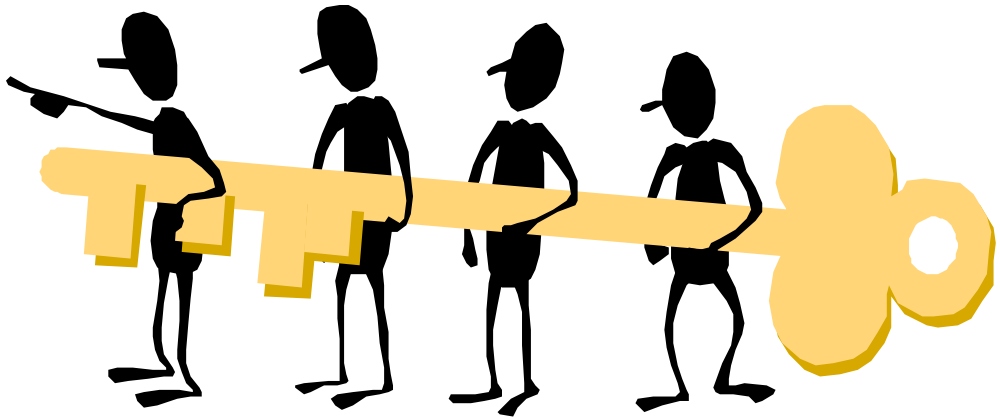
Location Management im GSM

- ***Grundprinzip verteilte Speicherung***
  - Verteilte Speicherung über Register
    - *Home Location Register* und *Visitor Location Register*
  - Netzbetreiber hat stets globale Sicht auf Daten
  - Bewegungsprofile sind erstellbar

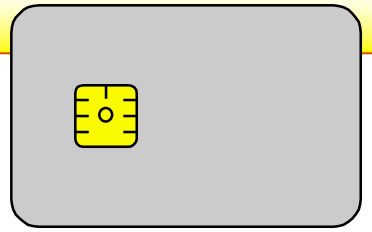


Sicherheitsrelevante Funktionen des GSM

- *Überblick*
  - **Subscriber Identity Module** (SIM, Chipkarte)
    - Zugangskontrolle und Kryptoalgorithmen
  - **einseitige Authentikation** (Mobilstation vor Netz)
    - Challenge-Response-Verfahren (Kryptoalgorithmus: A3)
  - **Pseudonymisierung der Teilnehmer** auf der Funkschnittstelle
    - Temporary Mobile Subscriber Identity (TMSI)
  - **Verbindungsverschlüsselung** auf der Funkschnittstelle
    - Schlüsselgenerierung: A8
    - Verschlüsselung: A5



Subscriber Identity Module (SIM)



- **Spezielle Chipkarte mit Rechenkapazität**

Gespeicherte Daten:

– IMSI (interne Teilnehmerkennung)

– teilnehmerspezifischer symmetrischer Schlüssel Ki (Shared Secret Key)

– PIN (Personal Identification Number) für Zugangskontrolle

– TMSI

– LAI

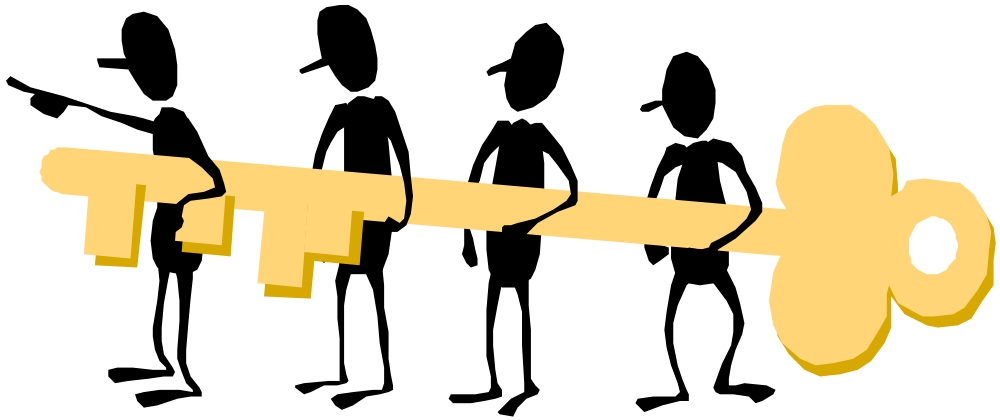
Krypto-Algorithmen:

– Algorithmus A3 für Challenge-Response-Authentikationsverfahren

– Algorithmus A8 zur Generierung von Kc (Session Key)

Sicherheitsrelevante Funktionen des GSM

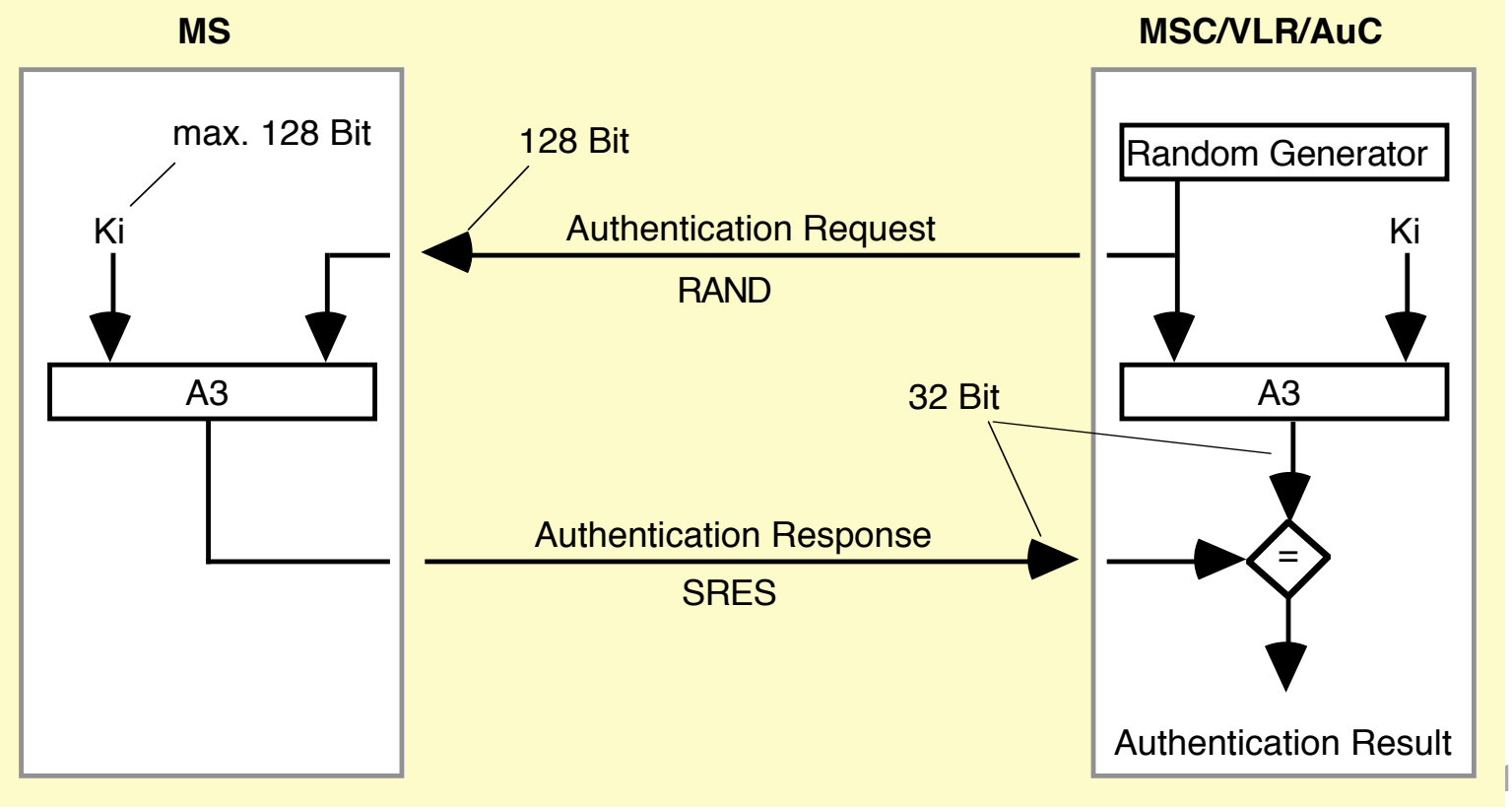
- *Überblick*
  - **Subscriber Identity Module** (SIM, Chipkarte)
    - Zugangskontrolle und Kryptoalgorithmen
  - **einseitige Authentikation** (Mobilstation vor Netz)
    - Challenge-Response-Verfahren (Kryptoalgorithmus: A3)
  - **Pseudonymisierung der Teilnehmer** auf der Funkschnittstelle
    - Temporary Mobile Subscriber Identity (TMSI)
  - **Verbindungsverschlüsselung** auf der Funkschnittstelle
    - Schlüsselgenerierung: A8
    - Verschlüsselung: A5



Challenge-Response-Authentikation

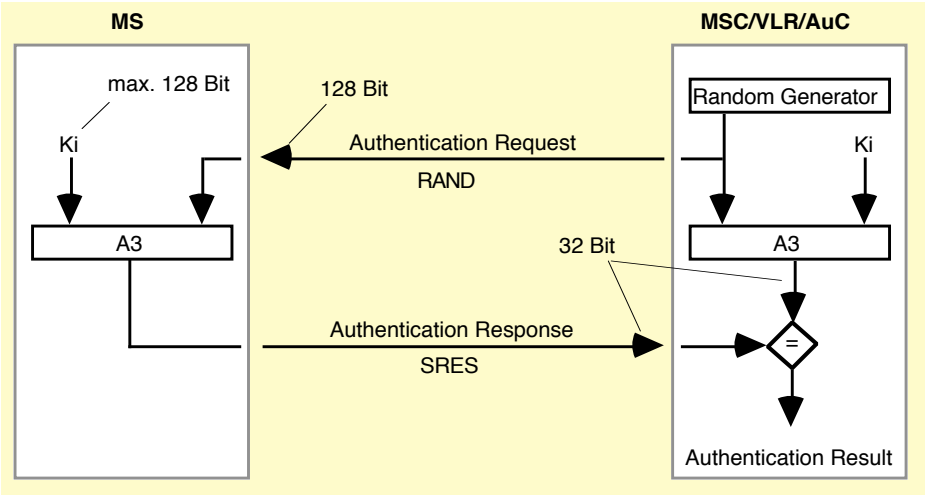
- ***Wann vom Netz initiiert?***
  - Aufenthaltsregistrierung (Location Registration)
  - Aufenthaltswechsel (Location Update) mit VLR-Wechsel
  - Call Setup (in beiden Richtungen)
  - Kurznachrichtendienst SMS (Short Message Service)

- ***Protokoll***



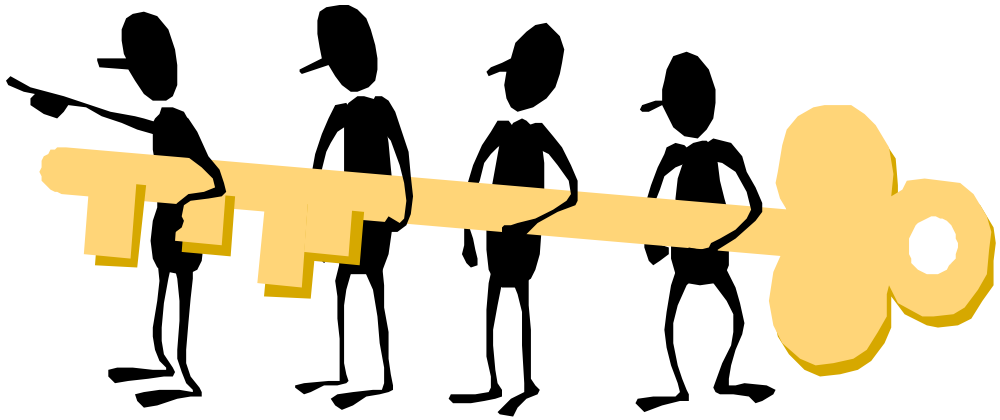
Challenge-Response-Authentikation

- ***Algorithmus A3***
  - auf SIM und im AuC untergebracht
  - mit Ki parametrisierte Einwegfunktion
  - nicht (europaweit, weltweit) standardisiert
  - kann vom Netzbetreiber festgelegt werden:
    - Authentikationsparameter werden vom Netzbetreiber an das prüfende (d.h. das besuchte) MSC übermittelt
    - dort lediglich Vergleichsoperation
    - besuchtes MSC muß der Güte von A3 vertrauen
  - Schnittstellen sind standardisiert



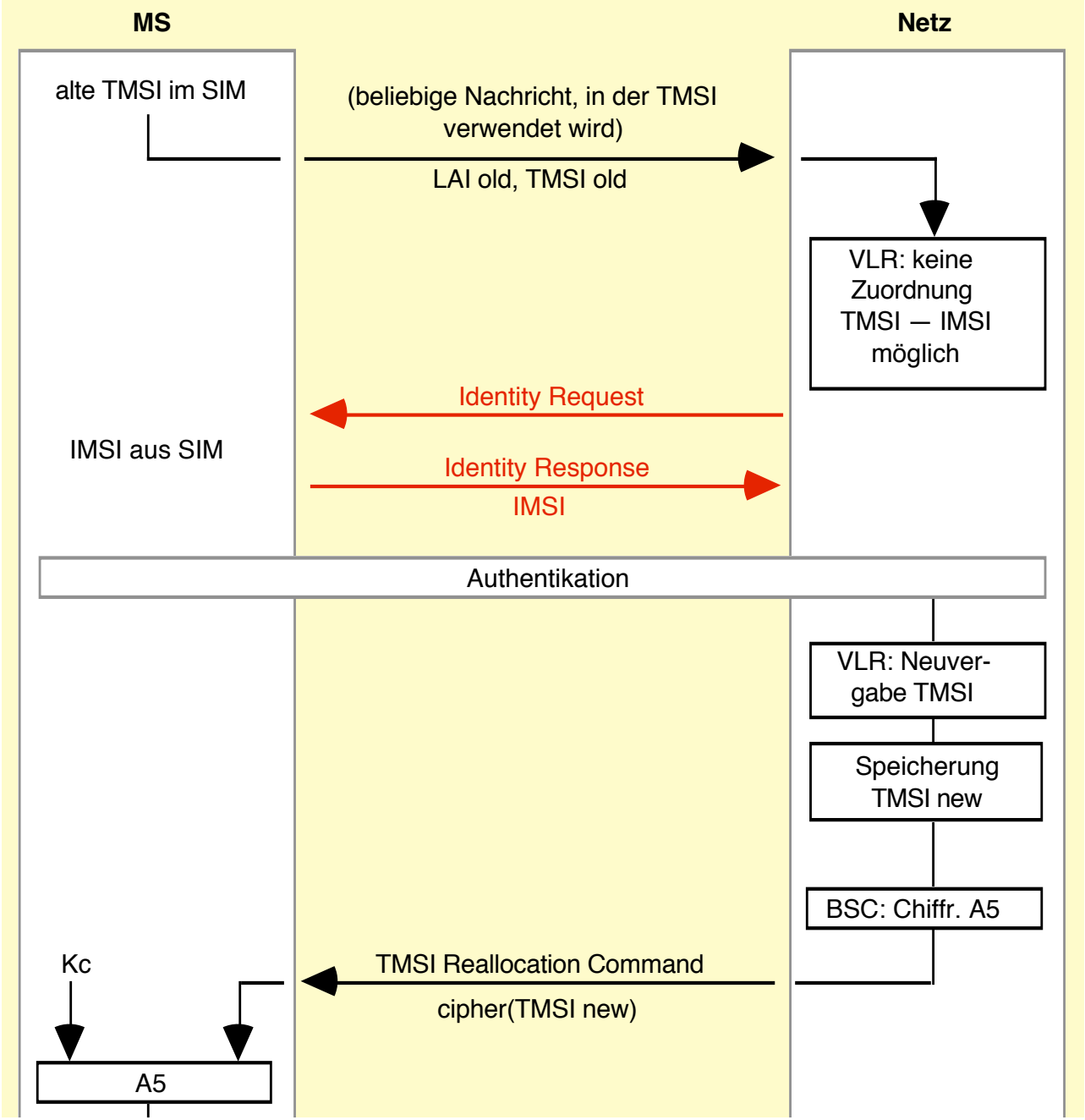
Sicherheitsrelevante Funktionen des GSM

- *Überblick*
  - **Subscriber Identity Module** (SIM, Chipkarte)
    - Zugangskontrolle und Kryptoalgorithmen
  - **einseitige Authentikation** (Mobilstation vor Netz)
    - Challenge-Response-Verfahren (Kryptoalgorithmus: A3)
  - **Pseudonymisierung der Teilnehmer** auf der Funkschnittstelle
    - Temporary Mobile Subscriber Identity (TMSI)
  - **Verbindungsverschlüsselung** auf der Funkschnittstelle
    - Schlüsselgenerierung: A8
    - Verschlüsselung: A5



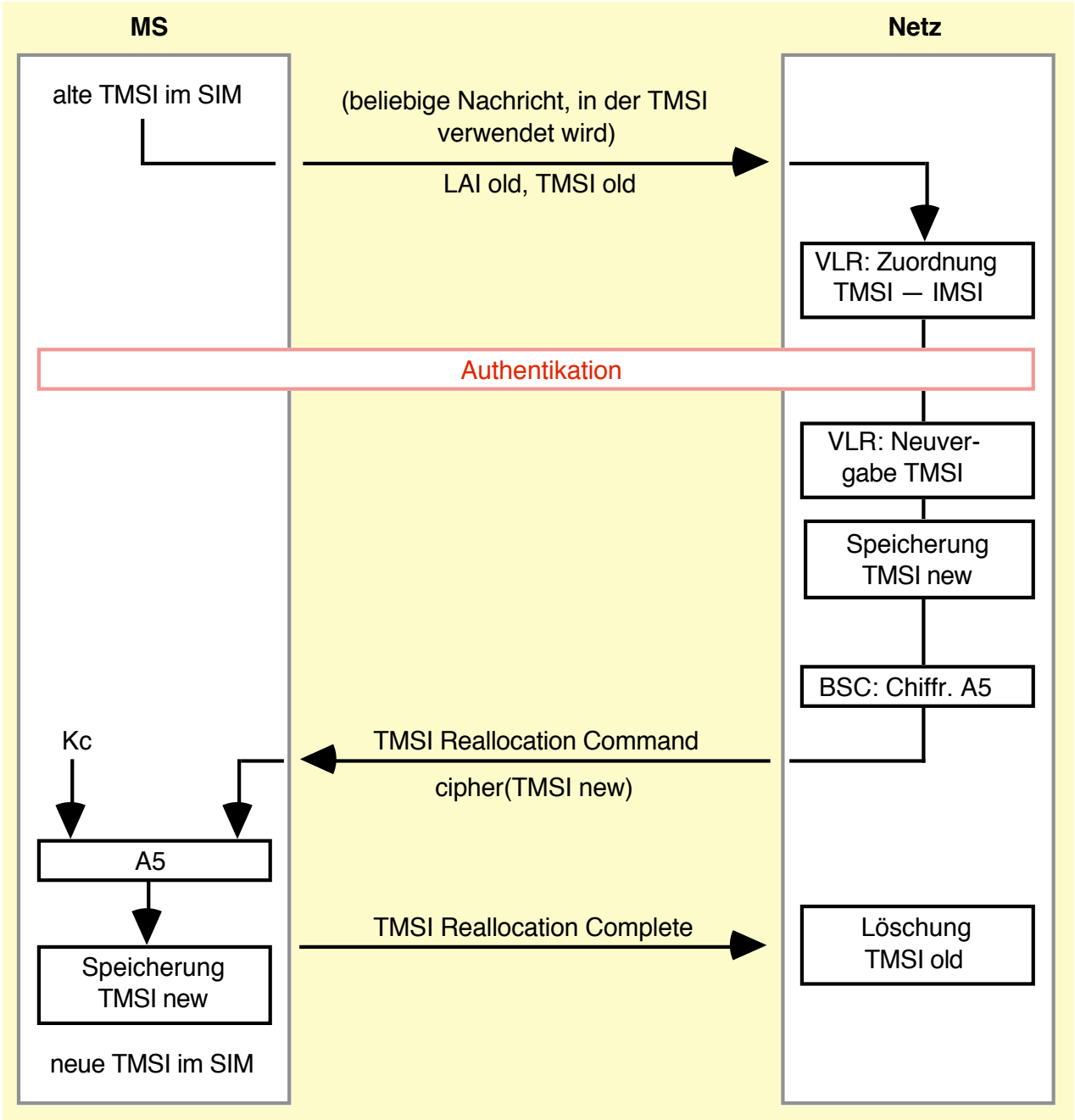
Pseudonymisierung auf der Funkschnittstelle

- ***TMSI (Temporary Mobile Subscriber Identity)***
  - soll Verkettung von Teilnehmeraktionen verhindern
  - Algorithmus zur Generierung der TMSI legt Netzbetreiber fest
  - bei erster Meldung (oder nach Fehler) wird IMSI übertragen
- ***Neuvergabe einer TMSI bei unbekannter alter TMSI***
  - Identity Request
  - ... kann jederzeit von Netz gesendet werden



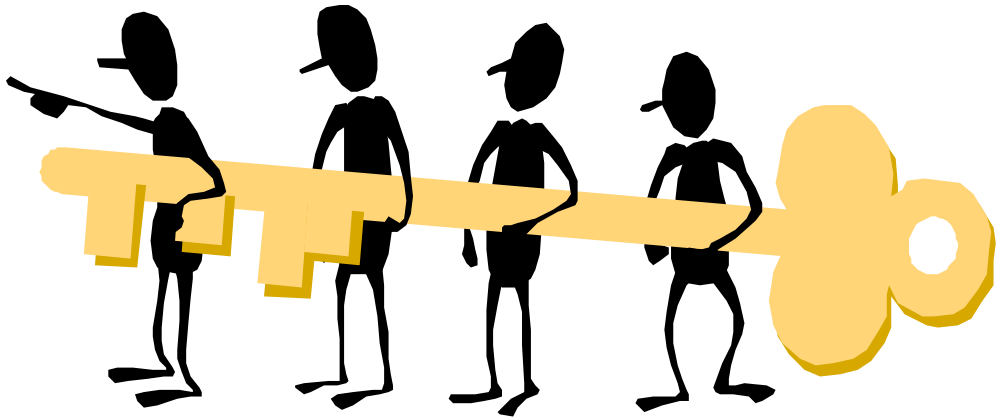
Pseudonymisierung auf der Funkschnittstelle

- ***TMSI (Temporary Mobile Subscriber Identity)***
  - soll Verkettung von Teilnehmeraktionen verhindern
  - Algorithmus zur Generierung der TMSI legt Netzbetreiber fest
  - bei erster Meldung (oder nach Fehler) wird IMSI übertragen



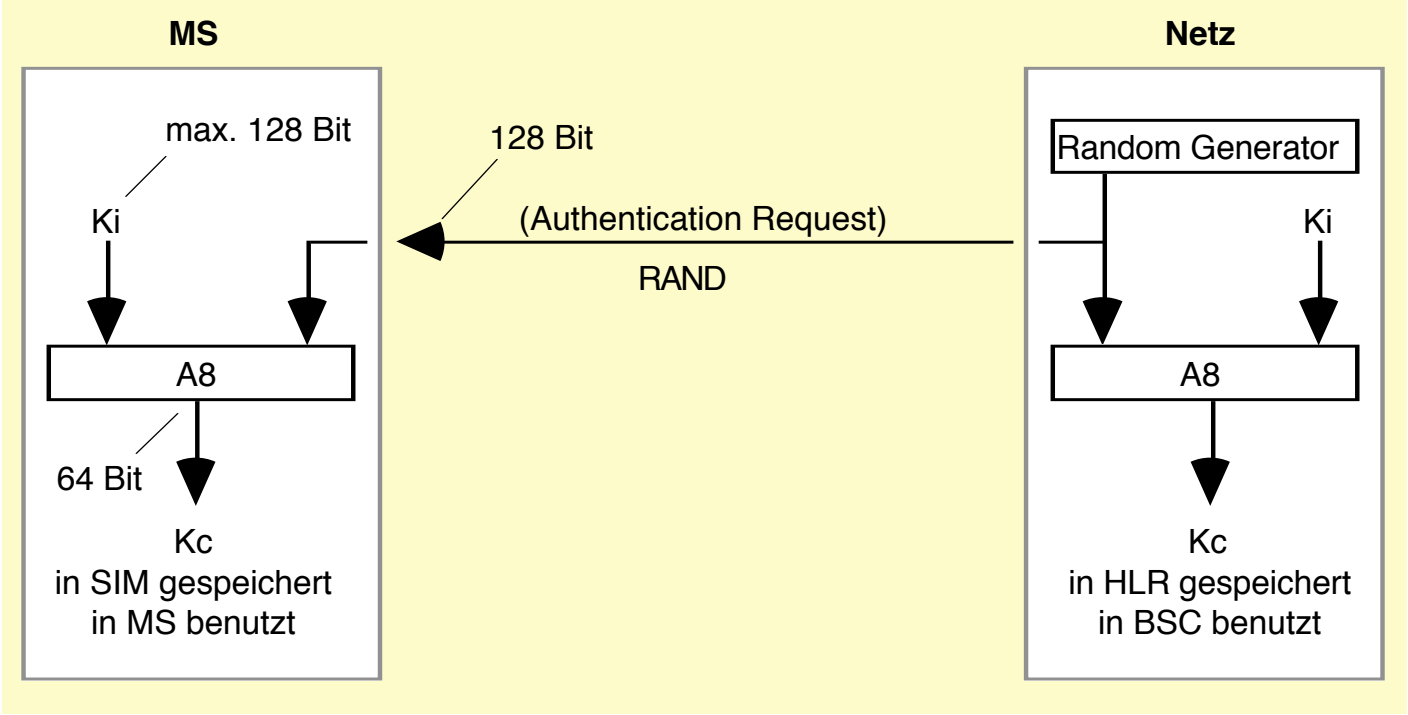
Sicherheitsrelevante Funktionen des GSM

- *Überblick*
  - **Subscriber Identity Module** (SIM, Chipkarte)
    - Zugangskontrolle und Kryptoalgorithmen
  - **einseitige Authentikation** (Mobilstation vor Netz)
    - Challenge-Response-Verfahren (Kryptoalgorithmus: A3)
  - **Pseudonymisierung der Teilnehmer** auf der Funkschnittstelle
    - Temporary Mobile Subscriber Identity (TMSI)
  - **Verbindungsverschlüsselung** auf der Funkschnittstelle
    - Schlüsselgenerierung: A8
    - Verschlüsselung: A5



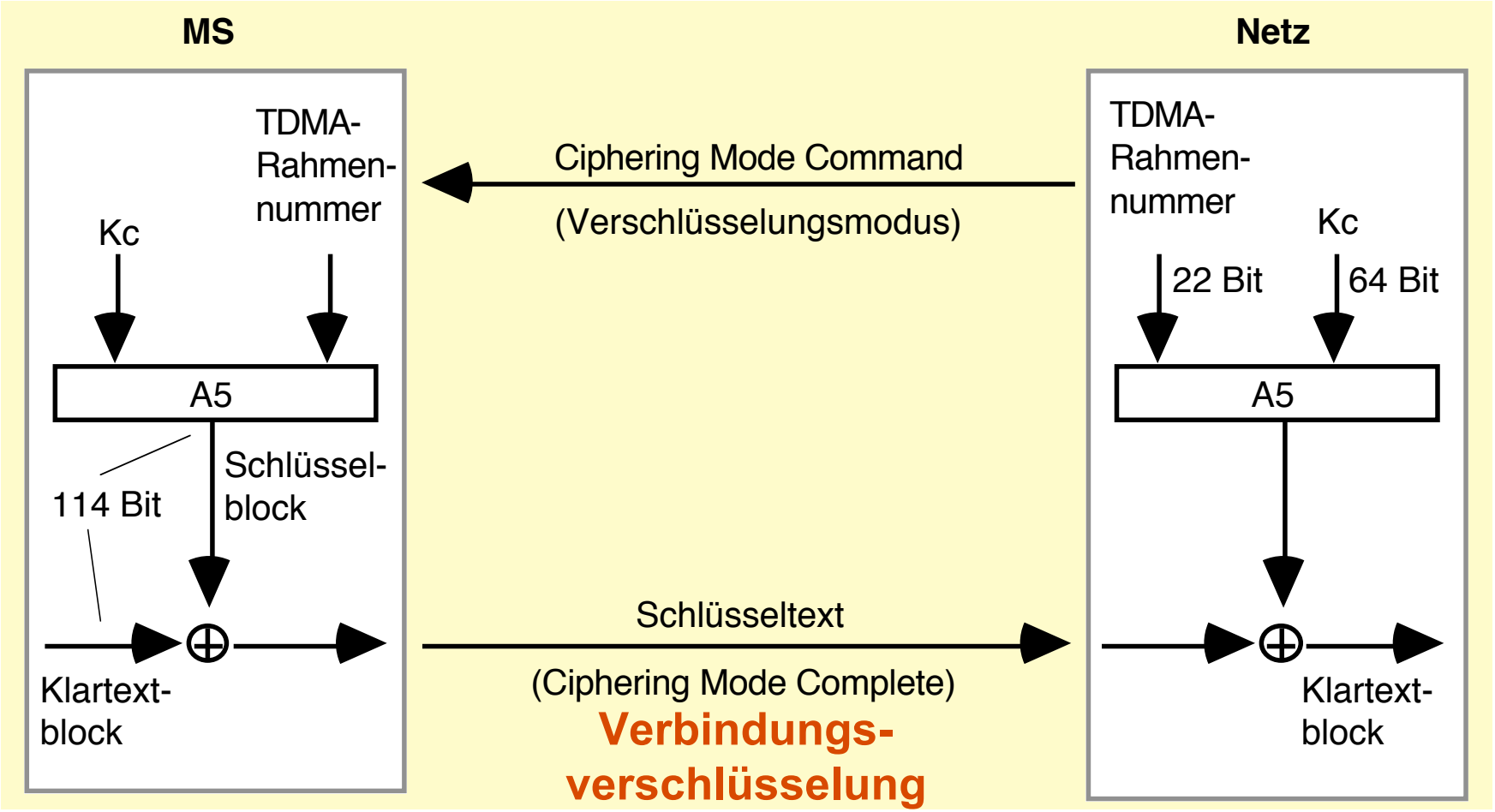
Verschlüsselung auf der Funkschnittstelle

- **Schlüsselgenerierung: Algorithmus A8**
  - auf SIM und im AuC untergebracht
  - mit Ki parametrisierte Einwegfunktion
  - nicht (europaweit, weltweit) standardisiert
  - kann vom Netzbetreiber festgelegt werden
  - Schnittstellen sind standardisiert
  - Kombination A3/A8 bekannt als COMP128



Verschlüsselung auf der Funkschnittstelle

- **Datenverschlüsselung: Algorithmus A5**
  - in der Mobilstation (nicht im SIM !) untergebracht
  - europa- bzw. weltweit standardisiert
  - schwächerer Algorithmus A5* oder A5/2 für bestimmte Staaten



Verschlüsselung auf der Funkschnittstelle

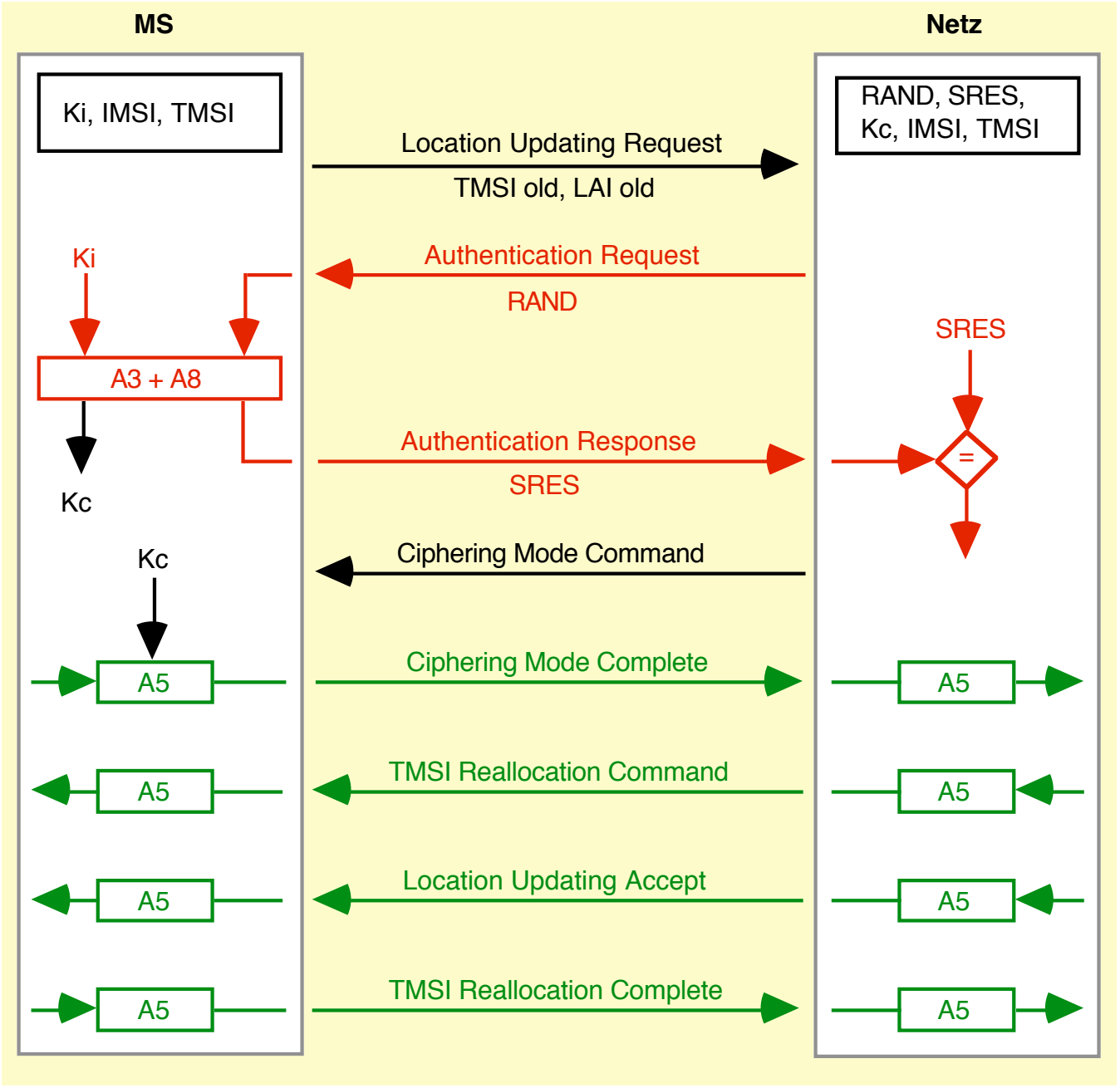
- *Ciphering Mode Command (GSM 04.08)*

Informationselement	Länge in Bit
Protocol discriminator Transaction discriminator Message type	16
Ciphering mode setting	8

- *Cipher mode setting information element*

8	7	6	5	4	3	2	1	
1	0	0	1	0	0	0	SC=0	**No chiphering**
	Ciph mode set IEI			Spare	Spare	Spare	SC=1	**Start ciphering**

Zusammenspiel der Sicherheitsfunktionen



Angriffe

- ***Kritik***
  - kryptographische Mechanismen geheim, also nicht «wohluntersucht»
    - Folge: Schwächen nicht auszuschließen
    - Angriff: SIM-Cloning
  - symmetrisches Verfahren
    - Folge: Speicherung nutzerspezifischer geheimer Schlüssel beim Netzbetreiber erforderlich
    - Angriff: «Abfangen» von Authentication Triplets
  - keine gegenseitige Authentikation vorgesehen
    - Folge: Angreifer kann ein GSM-Netz vortäuschen
    - Angriff: IMSI-Catcher

«SIM-Cloning»

- ***Angriffsziel***
  - Telefonieren auf Kosten anderer Teilnehmer
  - beschrieben von Marc Briceno (Smart Card Developers Association), Ian Goldberg und Dave Wagner (beide University of California in Berkeley)
  - http://www.isaac.cs.berkeley.edu/isaac/gsm.html
  - Angriff bezieht sich auf Schwäche des Algorithmus COMP128, der A3/A8 implementiert
  - SIM-Karte (incl. PIN) muß sich in zeitweiligem Besitz des Angreifers befinden
- ***Aufwand***
  - ca. 150.000 Berechnungsschritte, um Ki (max. 128 Bit) zu ermitteln
  - derzeit ca. 8 - 12 Stunden

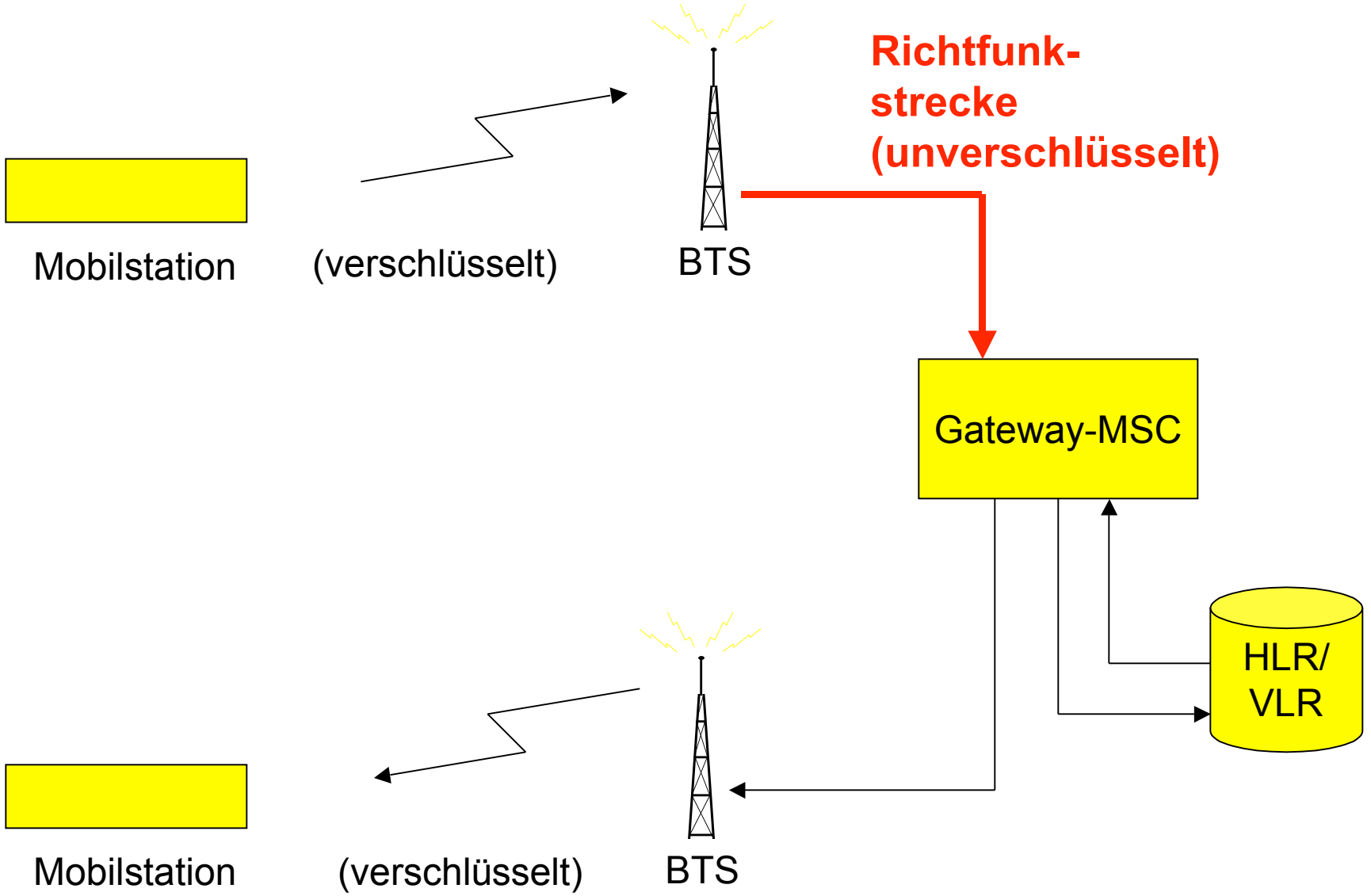
Angriffe

- ***Kritik***
  - kryptographische Mechanismen geheim, also nicht «wohluntersucht»
    - Folge: Schwächen nicht auszuschließen
    - Angriff: SIM-Cloning
  - symmetrisches Verfahren
    - Folge: Speicherung nutzerspezifischer geheimer Schlüssel beim Netzbetreiber erforderlich
    - Angriff: «Abfangen» von Authentication Triplets
  - keine gegenseitige Authentikation vorgesehen
    - Folge: Angreifer kann ein GSM-Netz vortäuschen
    - Angriff: IMSI-Catcher

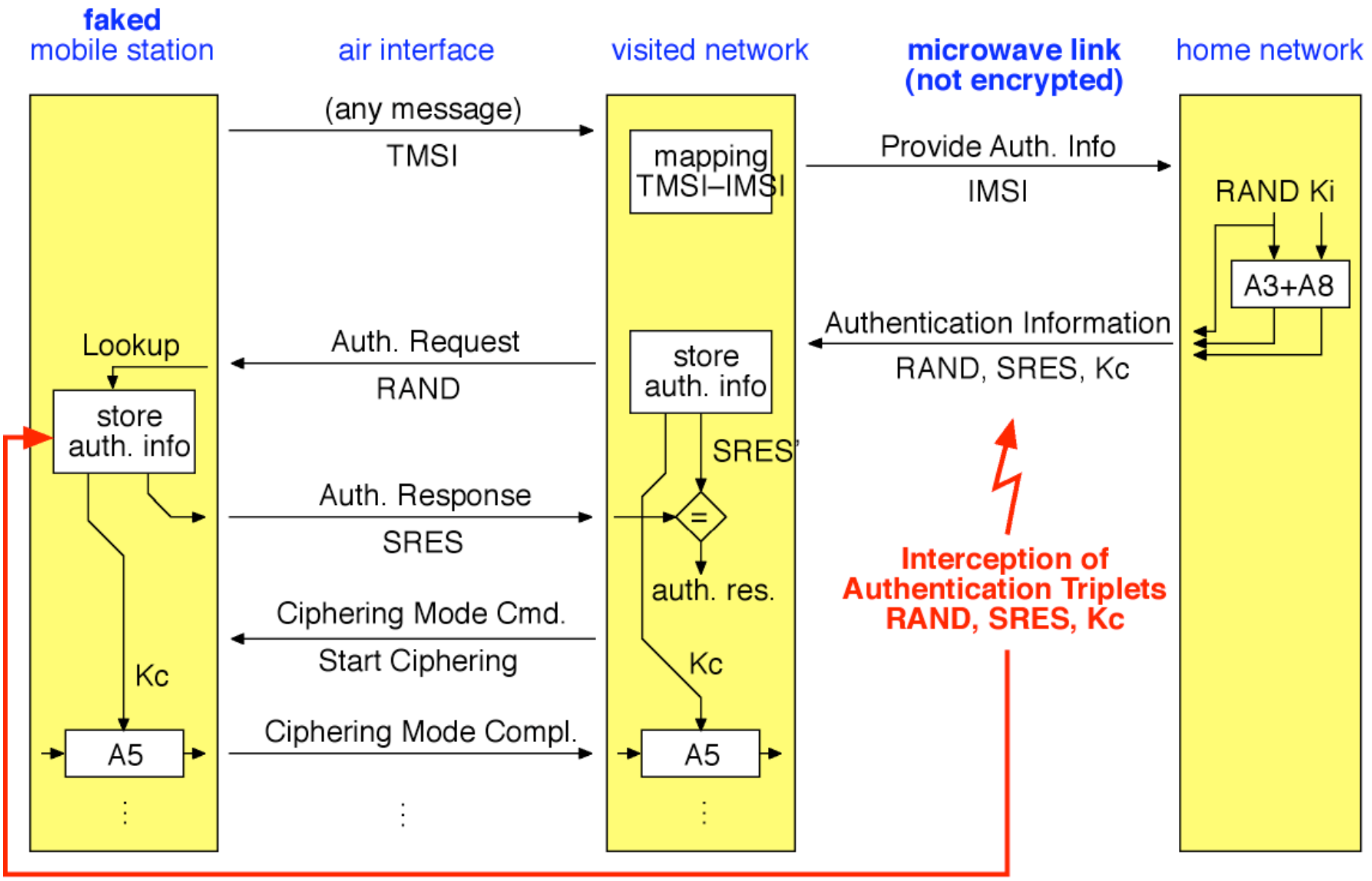
«Abfangen» von Authentication Sets

- ***Angriffsziel***
  - Telefonieren auf Kosten anderer Teilnehmer
  - beschrieben von Ross Anderson (Universität Cambridge)
  - Abhören der unverschlüsselten netzinternen Kommunikation bei Anforderung der Authentication Triples vom AuC durch das besuchte VLR/MSC
- ***Angriff beruht auf folgender «Schwäche»***
  - GSM-Standard beschreibt größtenteils Implementierung von Schnittstellen zwischen den Netzkomponenten
  - Verschlüsselung der Authentication Sets bei Übermittlung vom AuC zum VLR/MSC nicht vorgesehen

Verschlüsselung auf der Funkschnittstelle



«Abfangen» von Authentication Sets

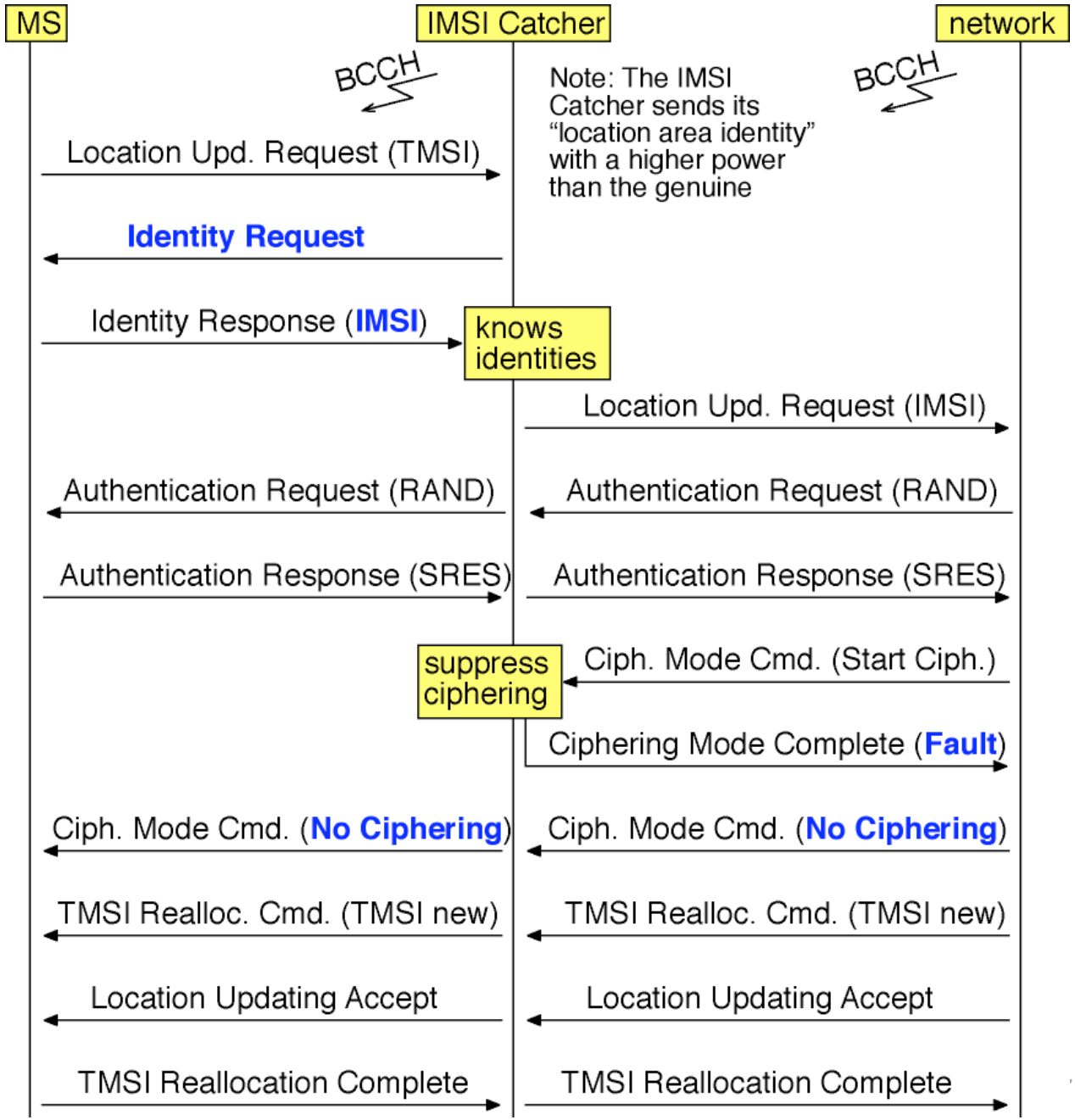


Angriffe

- ***Kritik***
  - kryptographische Mechanismen geheim, also nicht «wohluntersucht»
    - Folge: Schwächen nicht auszuschließen
    - Angriff: SIM-Cloning
  - symmetrisches Verfahren
    - Folge: Speicherung nutzerspezifischer geheimer Schlüssel beim Netzbetreiber erforderlich
    - Angriff: «Abfangen» von Authentication Triplets
  - keine gegenseitige Authentikation vorgesehen
    - Folge: Angreifer kann ein GSM-Netz vortäuschen
    - Angriff: IMSI-Catcher

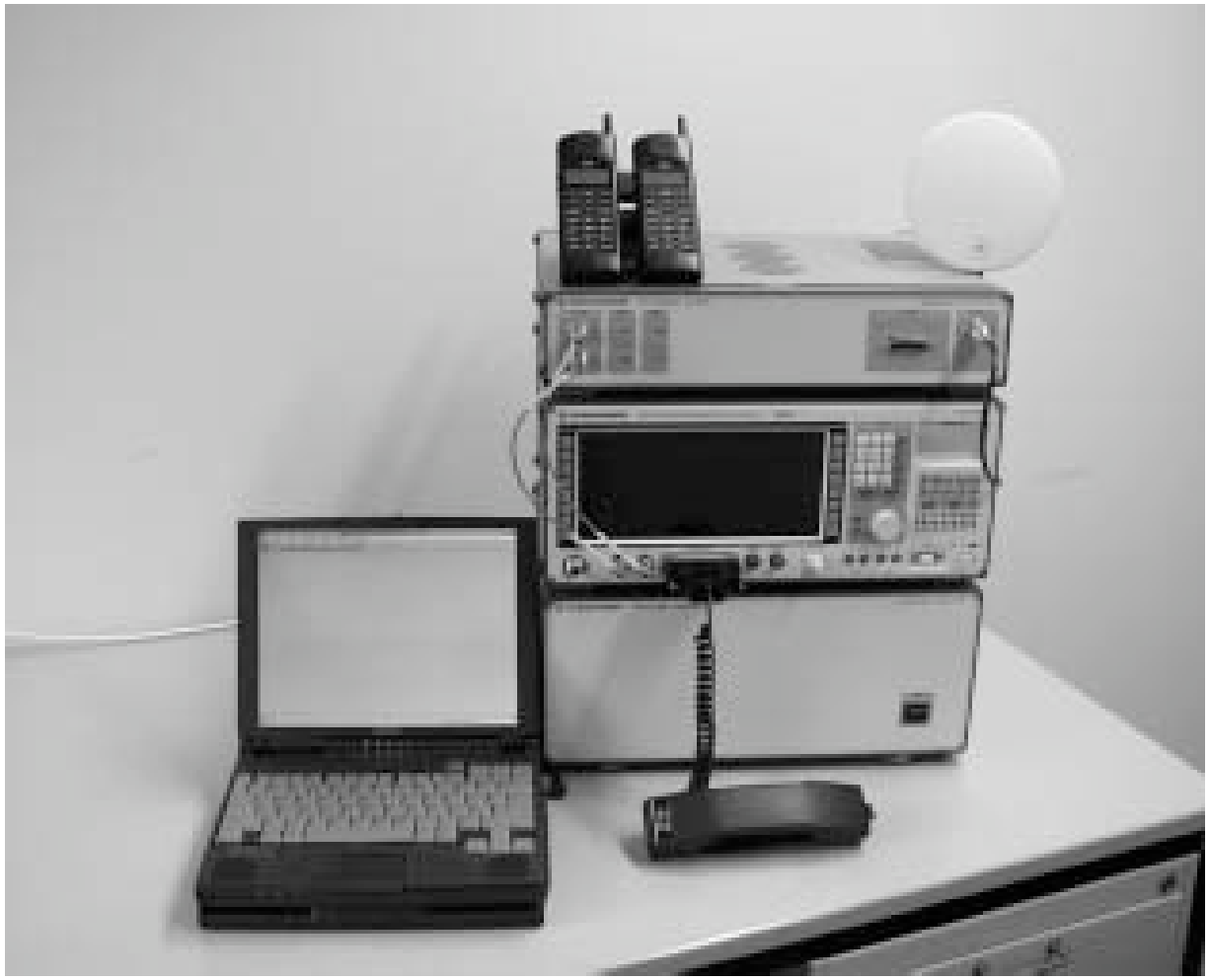
IMSI-Catcher

- ***Angriffsziele***
  - Welche Teilnehmer halten sich in der Funkzelle auf?
  - Gespräche mithören
- ***Man-in-the-middle attack (Maskerade)***
- ***Abwehr:***
  - Gegenseitige Authentikation:
    MS — Netz
    und
    Netz — MS



IMSI-Catcher

- ***Angriffsziele***
  - Welche Teilnehmer halten sich in der Funkzelle auf?
  - Gespräche mithören
- ***Man-in-the-middle attack (Maskerade)***
- ***Abwehr:***
  - Gegenseitige Authentikation:
    MS — Netz
    und
    Netz — MS



Quelle: Verfassungsschutz,
http://www.datenschutz-und-datensicherheit.de/jhrg26/imsicatcher-fox-2002.pdf

Zusammenfassung

- ***Datenschutzdefizite (Auswahl)***
  - geheimgehaltene symmetrische Kryptoverfahren
  - schwacher Schutz des Ortes gegen Outsider
  - kein Schutz gegen Insiderangriffe (Inhalte, Aufenthaltsorte)
  - keine Ende-zu-Ende-Dienste (Authentikation, Verschlüsselung)
  - Vertrauen des Nutzers in korrekte Abrechnung ist nötig
  - keine anonyme Netzbenutzung möglich
- ***Fazit: Stets werden externe Angreifer betrachtet.***
  - GSM soll lediglich das Sicherheitsniveau existierender Festnetze erreichen.

Sicherheit mobiler Systeme

- ***Ausblick***
  - Konzepte zur anonymen und unbeobachtbaren Kommunikation
  - Bezahlung mobiler Dienstleistungen
  - Sicherheit von Location-Based Services

http://www-sec.uni-regensburg.de